UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

KENNETH HENSLEY, as legal guardian of R.H., individually and on behalf of all others similarly situated, Plaintiff, v. MCG HEALTH, LLC, a Washington limited liability company, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kenneth Hensley, as legal guardian of R.H. ("Plaintiff"), individually and on behalf of all others similarly situated, and by and through his undersigned counsel files this Class Action Complaint against Defendant MCG Health, LLC ("MCG Health" or "Defendant") and alleges the following based upon personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Defendant provides patient care guidelines to health care providers and health plans, including care strategies, consulting, analytics, and other services. In this role, Defendant operates as a business associate as defined by the Health Insurance Portability and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Accountability Act ("HIPAA") and is required to comply with HIPAA regulations. *See* 45 CFR 160.103.

2. To provide its services, MCG requires its customers and their patients to provide MCG Health with sensitive and private information, including personally identifiable information ("PII") and protected health information ("PHI").

3. By taking possession and control of Plaintiff's and Class members' PHI and PII, Defendant assumes a duty to securely store and protect that sensitive information.

4. Defendant breached this duty and betrayed the trust of its clients, R.H. and Class members, by failing to properly safeguard and protect their PHI and PII, thus enabling cybercriminals to steal and misuse it.

5. With this action, Plaintiff and the Class seek to hold Defendant responsible for the harms it caused them resulting from the massive and preventable disclosure of such sensitive and personal information.

6. On March 25, 2022, MCG Health determined that cybercriminals had previously gained unauthorized access to its systems and acquired confidential personal information about patients and members whose information was stored on MCG Health's systems (the "Data Breach"). The patient and member information obtained by cybercriminals includes: names, dates of birth, Social Security numbers, medical codes, addresses, telephone numbers, email addresses, gender, and potentially other PII and PHI collected and stored by Defendant.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

7. Following a forensic investigation, MCG Health determined that cybercriminals accessed and acquired the PII and PHI of approximately 1,100,000 patients and members during the Data Breach.[1]

8. As a result of Defendant's negligent and wrongful conduct, Plaintiff's and Class members' highly confidential and sensitive PII and PHI was left exposed to cybercriminals.

9. Defendant's misconduct – failing to implement adequate and reasonable data security measures to protect Plaintiff's and Class members' PHI and PII, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices and employee training in place to safeguard the PHI and PII, failing to honor its promises and representations to protect Plaintiff's and Class members' PHI and PII, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

10. Due to Defendant's negligence and data security failures, cyber criminals had access to and now potentially possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of 1,100,000 individuals.

11. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that Plaintiff's PHI and PII has been released into the hands of cybercriminals, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and fraudulently using their PHI and PII.

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/1948d82a-0cdb-4b37-a988-b4189351176b.shtml.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff and Class members have lost time and money responding to and attempting to mitigate the impact of the Data Breach.

12. Plaintiff brings this action individually and on behalf of the Class and seek actual damages, statutory damages, treble damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

THE PARTIES

13. Plaintiff is a citizen and resident of the state of Van Buren, Indiana.

14. Defendant is a Washington limited liability company with its principal place of business at 901 Fifth Avenue, Suite 120, Seattle, WA 98164.

JURISDICTION AND VENUE

15. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendant.

16. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Washington and this District through its headquarters and offices.

17. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

FACTUAL ALLEGATIONS

A. The Data Breach

18. Defendant is at a minimum a business associate of various health care providers and is in receipt of highly sensitive PHI and PII. As such, Defendant is required pursuant to Federal and State law to maintain the strictest confidentiality of its patients and the PHI and PII it receives and collects, and Defendant is further required to maintain sufficient safeguards to protect such PHI and PII from being accessed by unauthorized third parties.

19. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant recognizes privacy rights, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in this Data Breach.

20. Defendant promises to maintain the confidentiality of Class members' PHI and PII to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class members' PII or PHI for any reasons other than those expressly listed in the Privacy Notice without written authorization.

21. As a condition of receiving Defendant's services, Defendant requires that Plaintiff and Class members entrust it with highly sensitive personal information.

22. On March 25, 2022, MCG Health determined that cybercriminals had previously gained unauthorized access to its systems and ***acquired*** confidential personal information about patients and members whose information was stored on Defendant's systems.

23. In the letter sent to Class members, Defendant acknowledges that "an unauthorized party previously obtained certain of your personal information that matched data

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

stored on [Defendant's] systems. The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender."[2]

24. Based on Defendant's acknowledgement that the PHI and PII was "obtained" by cybercriminals, it is evident that unauthorized cybercriminals did in fact access Defendant's files, and exfiltrated Plaintiff's and Class members' PHI and PHI from those files.

25. On information and belief, the PHI and PII contained in the files accessed by cybercriminals was not encrypted.

26. On information and belief, the cyberattack was targeted at Defendant due to its status as a HIPAA associated business entity that collects, creates, and maintains PHI and PII.

27. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PHI and PII of patients and/or members, like Plaintiff and the Class members.

28. Moreover, while Defendant admits that it learned of the Data Breach in March 2022, Defendant inexplicably waited two and a half months after determining that cybercriminals had in fact obtained Plaintiff's and Class member's information in the Data Breach before Defendant began the process of notifying impacted patients, such as Plaintiff and Class members.[3]

29. Apparently, Defendant needed more than two months following the completion of its investigation to notify the impacted individuals of the Data Breach and of the need for them to

[2] https://www.mcg.com/wp-content/uploads/2022/06/MCG-Website-Notice_90273447_1-6.8.22481312.4-004.pdf.
[3] *See id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

protect themselves against fraud and identity theft. Defendant was, of course, too late in the discovery and notification of the Data Breach.

30. Due to Defendant's inadequate security measures and its delayed notice to victims, Plaintiff and the Class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

31. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class members to keep their PHI and PII confidential and to protect it from unauthorized access and disclosure.

32. Plaintiff and Class Members provided their PHI and PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII and PHI from unauthorized disclosure.

34. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and Class members would not have entrusted Defendant with their PII and PHI had they known that Defendant would fail to implement industry standard protections for that sensitive information.

35. As a result of Defendant's negligent and wrongful conduct, Plaintiff's and Class members' highly confidential and sensitive PII and PHI was left exposed to cybercriminals.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

B. Plaintiff's Experience

36. Plaintiff received a letter from MCG Health dated June 10, 2022, advising that his minor child R.H.'s information was acquired by cybercriminals in the Data Breach. *See* Exhibit 1, attached hereto. The letter advised that the information of R.H.'s that has been compromised in the Data Breach includes some or all of the following PII and PHI: name, Social Security number, date of birth, medical codes, postal address, telephone numbers, email addresses, and gender.

37. As required in order to obtain medical services, Plaintiff provided R.H.'s highly sensitive personal and health information, including the PHI and PII that was compromised in the Data Breach.

38. Because of Defendant's negligence and failure to properly secure the PII and PHI in its possession, which negligence and failure led to the Data Breach, R.H.'s PHI and PII have been obtained by cybercriminals.

39. R.H. is now under an imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of R.H.'s life. The imminent risk of identity theft and fraud R.H. now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendant in its failure to implement adequate data security protocols, which negligence led to the Data Breach.

40. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for R.H., including investigating the Data Breach,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

investigating how best to ensure that R.H. is protected from identity theft, and securing identity theft protection services for R.H.

41. As a direct and proximate result of the Data Breach, Plaintiff will need to have identity theft protection for the rest of R.H.'s lifetime.

42. R.H. has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of R.H.'s PHI and PII that was entrusted to Defendant for the sole purpose of obtaining medical services necessary for R.H.'s health and well-being, with the understanding that Defendant would safeguard this information against unauthorized disclosure. Additionally, R.H.'s PHI and PII is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendant and is subject to future wrongful disclosures and/or security breaches so long as Defendant fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

C. Defendant Had an Obligation to Protect PHI and PII under Federal Law and the Applicable Standard of Care

43. Defendant is covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

44. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[4] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

45. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

46. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

47. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

48. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

49. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

[4] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

50. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

51. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

52. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[5]

53. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the

[5] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

54. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

55. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[6] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[7]

56. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure

[6] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[7] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

57. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI and PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PHI and PII of the Class.

58. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the PHI and PII in its possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect PHI and PII.

59. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a compromise of PHI and PII in a timely manner.

60. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

61. Defendant owed a duty to Plaintiff and the Class to disclose whether its computer systems and data security practices were inadequate to safeguard individuals' PHI and PII from theft because such an inadequacy would be a material fact in the decision to entrust PHI and PII with Defendant.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

62. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

63. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

D. Defendant was on Notice of Data Threats in the Healthcare Industry and of the Inadequacy of its Data Security

64. Defendant was on notice that companies in the healthcare industry are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information.

65. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[8]

66. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[9]

[8] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[9] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

67. As implied by the above AMA quote, stolen PHI and PII can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class members.

68. Defendant was on notice that the federal government has been concerned about healthcare company data encryption. Defendant knew its employees kept protected health information in their personal files, yet it appears that information was not encrypted.

69. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[10]

70. As a covered entity under HIPAA, Defendant should have known about its data security vulnerabilities and sought better protection for the PHI and PII accumulating in its employees' unprotected files.

E. Cyber Criminals Will Use Plaintiff's and Class Members' PHI and PII to Defraud Them

71. Plaintiff's and Class members' PHI and PII is of great value to cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of

[10] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

72. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[11] For example, with the PHI and PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[12] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

73. PHI and PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[13]

74. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[14]

---

[11] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[12] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[14] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

75. The PHI and PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[15]

76. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

77. For instance, with a stolen Social Security number, which is only one category of the PHI and PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[17]

78. Identity thieves can also potentially use the information stolen from Plaintiff and Class members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and

---

[15] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.
[16] *Data Breaches Are Frequent*, *supra* note 11.
[17] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

finance, the government and the military, or education.[18] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

79. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[20]

80. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

81. Plaintiff and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

---

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.
[19] *Id.*
[20] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Trespass, damage to, and theft of their personal property, including PHI and PII;

b. Improper disclosure of their PHI and PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PHI and PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PHI and PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

82. Moreover, Plaintiff and Class members have an interest in ensuring that their PHI and PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's and Class members' PHI and PII.

83. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the kind of PHI and PII Defendant made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PHI and PII, Plaintiff and Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[21]

84. None of this should have happened. The Data Breach was entirely preventable.

F. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' PHI and PII

85. Data disclosures and data breaches are preventable.[22] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[23] She added that "[o]rganizations that collect,

[21] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[22] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[23] *Id.* at 17.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[24]

86. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[25]

87. Defendant required Plaintiff and Class members to surrender their PHI and PII – including but not limited to their names, addresses, Social Security numbers, dates of birth, medical codes, email addresses, and gender – and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PHI and PII.

88. Defendant breached fiduciary duties owed to Plaintiff and the Class as guardian of their PHI and PII.

89. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiff's and Class members' PHI and PII.

90. Defendant maintained the PHI and PII in an objectively reckless manner, making the PHI and PII vulnerable to unauthorized disclosure.

91. Defendant knew, or reasonably should have known, of the importance of safeguarding PHI and PII and of the foreseeable consequences that would occur if Plaintiff's and

[24] *Id.* at 28.
[25] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Class members' PHI and PII was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

92. The risk of improper disclosure of Plaintiff's and Class members' PHI and PII was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' PHI and PII from that risk left the PHI and PII in a dangerous condition.

93. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PHI and PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PHI and PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

94. Plaintiff brings this action under Federal Rule of Civil Procedure 23 against Defendant individually and on behalf of all others similarly situated. Plaintiff asserts all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose personally identifiable information and/or protected health information was accessed or acquired as a result of the MCG Health data breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around June 10, 2022 (the "Nationwide Class" or "Class").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

95. Excluded from the Nationwide Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

96. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

97. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

98. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable.

99. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PHI and PII compromised in the same way by the same conduct of Defendant.

100. Adequacy: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

101. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

102. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;
b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PHI and PII;
c. Whether Defendant's computer systems and data security practices used to protect Plaintiff's and Class members' PHI and PII violated the FTC Act and/or HIPAA, and/or state laws and/or Defendant' other duties discussed herein;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PHI and PII, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach or disclosure;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties to Plaintiff and the Class to use reasonable care in protecting their PHI and PII;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

j. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class;

l. Whether Defendant's actions and inactions alleged herein constitute gross negligence; and

m. Whether Plaintiff and Class members are entitled to treble damages.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of the Nationwide Class)

103. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

104. Defendant gathered and stored the PHI and PII of Plaintiff and the Class as part of the operation of its business.

105. Upon accepting and storing the PHI and PII of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

106. Defendant had full knowledge of the sensitivity of the PHI and PII, the types of harm that Plaintiff and Class members could and would suffer if the PHI and PII was wrongfully disclosed, and the importance of adequate security.

107. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their PHI and PII that was in Defendant' possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

108. Defendant owed Plaintiff and Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their PHI and PII, including taking action to reasonably

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

109. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

110. Defendant had duties to protect and safeguard the PHI and PII of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive PHI and PII. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' PHI and PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' PHI and PII in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PHI and PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

111. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the PHI and PII that had been entrusted to them.

112. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' PHI and PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PHI and PII in its possession;

b. Failing to protect the PHI and PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PHI and PII;

d. Failing to adequately train its employees to not store unencrypted PHI and PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PHI and PII;

f. Failing to mitigate the harm caused to Plaintiff and the Class members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their PHI and PII.

113. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

114. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

115. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PHI and PII of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PHI and PII of Plaintiff and Class members while it was within Defendant's possession and control.

116. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to securing their PHI and PII and mitigating damages.

117. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the PHI and PII, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

118. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

119. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

120. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of the Nationwide Class)

121. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

122. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the PHI and PII of Plaintiff and the Class.

123. Defendant is a covered entity under HIPAA, 45 C.F.R. §160.102, and as such is required to comply with the HIPAA's Privacy Rule and Security Rule. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

124. HIPAA further requires Defendant to disclose the unauthorized access and theft of the protected health information of Plaintiff and the Class "without unreasonable delay" so that Plaintiff and Class members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404, 164.406, and 164.410.

125. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI and PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

126. Defendant gathered and stored the PHI and PII of Plaintiff and the Class as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

127. Defendant violated the FTC Act by failing to use reasonable measures to protect the PHI and PII of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

128. Defendant breached its duties to Plaintiff and the Class under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' PHI and PII, and by failing to provide prompt notice without reasonable delay.

129. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

130. Plaintiff and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

131. The harm that occurred as a result of the Data Breach is the type of harm HIPAA and the FTC Act were intended to guard against.

132. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PHI and PII.

133. Additionally, Defendant had a duty to promptly notify Plaintiff and the Class of the Data Breach. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

members of the Data Breach until June 10, 2022, despite knowing by March 25, 2022 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiff and the Class.

134. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

135. Defendant's violation of the FTC Act and HIPAA constitutes negligence *per se*.

136. As a direct and proximate result of Defendant' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

137. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

138. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of the Nationwide Class)

139. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

140. Defendant entered into various written contracts with its clients to perform services that include, but are not limited to, providing care strategies, consulting, analytics, and other services.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

141. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Indeed, Defendant knew that if it were to breach these contracts with its clients, the clients' patients or members – Plaintiff and Class members – would be harmed.

142. Defendant breached the contracts it entered into with its other clients by, among other things, failing to (i) use reasonable data security measures, and (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's PHI and PII from unauthorized disclosure to third parties.

143. As foreseen, Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

144. Plaintiff and Class members are also entitled to their costs and attorney's fees incurred in this action.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

145. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

146. Plaintiff and Class members bring this cause of action alternatively to their claim for breach of third-party beneficiary contract.

147. Plaintiff and Class members, as part of their agreements with Defendant, provided Defendant with their PHI and PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

148. In providing such PHI and PII, Plaintiff and Class members entered into implied contracts with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and Class members' PHI and PII.

149. Under the implied contracts, Defendant was obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and Class members with prompt, adequate notice of any data breach or unauthorized access of said information.

150. Defendant breached its implied contracts with Plaintiff and Class members by failing to take reasonable measures to safeguard the PHI and PII.

151. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' PHI and PII, Plaintiff and members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life, the untimely and/or inadequate notification of the Data Breach, improper disclosure of their PHI and PII, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach, the value of their time spent mitigating identity theft and/or identity fraud and/or increased risk of identity theft and/or identity fraud, and increased risk of identity theft and/or identity fraud.

FIFTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT (RCW 19.86.010 *ET SEQ.*)
(On Behalf of the Nationwide Class)

152. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

153. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

154. Defendant is a "person" as described in RWC 19.86.010(1).

155. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

156. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington.

157. In the course of conducting their business, Defendant committed "unfair acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices ongoing and continue to this date.

158. Defendant's conduct was also deceptive. Defendant failed to timely notify and concealing from Plaintiff and Class Members the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

information not been hidden from them, they could have taken precautions to safeguard and protect their PII, medical information, and identities.

159. Defendant's above-described "unfair or deceptive acts or practices" in violation effects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

160. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

161. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiff and Class Members' business and property. Plaintiff and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality his or her PII; (5) deprivation of the value of his or her PII, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them

162. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct and requiring Defendant to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

163. Plaintiff, on behalf of Plaintiff and the Class Members, also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of Plaintiff and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

SIXTH CAUSE OF ACTION
INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of the Nationwide Class)

164. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

165. Plaintiff and Class members reasonably expected that the sensitive PHI and PII entrusted to Defendant would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

166. Defendant unlawfully invaded the privacy rights of Plaintiff and Class members by:

a. Failing to adequately secure their sensitive PHI and PII from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

167. A reasonable person would find it highly offensive that Defendant, having collected Plaintiff's and Class members' sensitive PHI and PII, failed to protect such PHI and PII from unauthorized disclosure to third parties.

168. Indeed, such disclosure goes against the public policies of the State of Washington. For example, RCW 70.02.005 provides: "Persons other than health care providers obtain, use, and disclose health record information in many different contexts and for many different purposes. It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers."

169. In failing to adequately protect Plaintiff's and Class members' sensitive personal information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiff's and Class members' position.

170. Defendant violated Plaintiff's and Class members' right to privacy under the common law.

171. Defendant's unlawful invasions of privacy damaged Plaintiff and the Class. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiff and Class members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiff and the Class seek actual and nominal damages for these invasions of privacy.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

SEVENTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY
(On Behalf of the Nationwide Class)

172. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

173. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiff and the Class to keep Plaintiff's PHI and PII.

174. The fiduciary duty of privacy is explicated under the procedures set forth in RCW 70.02.270, which required Defendant to secure the health care information it maintains and to keep it free from disclosure.

175. Defendant breached its fiduciary duty to Plaintiff by disclosing Plaintiff's and other Class members' PHI and PII to unauthorized third parties.

176. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiff's confidential PHI and PII, Plaintiff and the Class members have suffered damages.

177. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' PHI and PII, Plaintiff and the Class have suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, and humiliation.

178. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of the PHI and PII; (iii) loss of privacy; (iv) out-of-pocket

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and (vii) emotional distress. At the very least, Plaintiff and the Class are entitled to nominal damages.

EIGHTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of the Nationwide Class)

179. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

180. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

181. As previously alleged, Plaintiff and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the PHI and PII it collected from Plaintiff and the Class.

182. Defendant owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' PHI and PII.

183. Defendant still possesses the PHI and PII of Plaintiff and the Class members.

184. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

185. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

further harm due to the exposure of their PHI and PII and Defendant's failure to address the security failings that led to such exposure.

186. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

187. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant provide employee training regarding the dangers and risks inherent in using file-sharing websites like the Website at issue here to store and/or transmit PHI and PII;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Ordering that Defendant cease transmitting PHI and PII via file-sharing websites like the Website at issue here;

f. Ordering that Defendant cease storing PHI and PII on file-sharing websites like the Website at issue here;

g. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PHI and PII not necessary for its provision of services;

h. Ordering that Defendant conduct regular database scanning and security checks; and

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, treble damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: July 15, 2022

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
Jason T. Dennett, WSBA #30686
s/ Rebecca L. Solomon
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
rsolomon@tousley.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

**pro hac vice request forthcoming*

Counsel for Plaintiff and the Putative Class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

EXHIBIT 1

MCG Health, LLC
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 10, 2022

H9734-L04-0233035 T00764 P015 ********SCH 5-DIGIT 46952
[redacted]

Dear [redacted]:

MCG Health, LLC ("MCG") provides patient care guidelines to health care providers and health plans. We are writing to notify you of a recent data security issue at MCG that affects certain of your personal information.

MCG determined on March 25, 2022 that an unauthorized party previously obtained certain of your personal information that matched data stored on MCG's systems. The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.

Upon learning of this issue, we took steps to understand its nature and scope. A leading forensic investigation firm was retained to assist in the investigation. Additionally, we are coordinating with the FBI. We have deployed additional monitoring tools and will continue to enhance the security of our systems.

We regret any concern this issue may cause. We are alerting you about this issue so you can take steps to help protect your information. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

In addition, we have arranged to offer you identity protection and credit monitoring services for two years at no cost to you through Experian's® IdentityWorks℠ services for minors. The attached Reference Guide provides information on activation and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We hope this information is useful to you. If you have questions regarding this issue, please call 1-866-475-7221 Monday – Friday, 6 am to 8 pm PT; Saturday – Sunday, 8 am to 5 pm PT.

Sincerely,

Jon Shreve

Jon Shreve
President and CEO

0233035

H9734-L04